SUDAN
Digital harms in conflict zones

ACAPS ANALYSIS HUB SUDAN
Thematic Report
15 December 2025

THREAT OVERVIEW

During conflict, digital technologies can become double-edged tools – important for affected people's safety and survival, necessary for information-sharing, and required for humanitarian coordination but simultaneously able to cause unintentional harm or be weaponised by conflict parties or other groups intent on causing harm to individuals, communities, humanitarian responders, or the international community. **Online harms can often become offline harms, mirroring or amplifying conflict dynamics** (CDAC 18/09/2025). As Sudan becomes more digitalised, conflict parties are increasingly using online spaces to control narratives and expand their support base, increasing the risks associated with the manipulation and control of digital technologies.

The weaponisation of digital technologies and the unintended effects of their use can lead to a range of diverse threats, including but not limited to technology-facilitated gender-based violence (TFGBV) and child sexual abuse material (CSAM); the polarisation of communities and threats to humanitarian responders stemming from coordinated disinformation, hate speech, and deepfakes; and deliberate internet shutdowns by armed parties that affect humanitarian access and operational continuity (TIMEP 14/01/2025; CDAC 18/09/2025; Amnesty International 08/03/2024; SIHA 20/01/2025; Hopes and Actions 13/01/2025).

Available evidence shows that the Rapid Support Forces (RSF), the Sudanese Armed Forces (SAF), and their supporters commit digital harms in Sudan. This growing threat affects various communities differently and ranges from targeted harassment and attacks, such as the online targeting of individual journalists and activists, to community-wide harms, such as misinformation and disinformation about conflict dynamics and region- or countrywide internet blackouts (Conven 20/07/2025; NRC 13/05/2024; Amnesty International 08/03/2024). That said, certain populations appear to be at heightened risk of targeted digital harm in Sudan, including women and girls, activists, and frontline humanitarian staff, who face overlapping risks when digital systems are weaponised.

The use of digital technologies in the early identification of the recent atrocities committed in Al Fasher – and their role in documenting and spreading evidence of RSF's and affiliated militias' crimes – highlights both the importance of digital technologies in documenting evidence and the effects of their weaponisation in conflict (Raymond et al. 27/10/2025; The Guardian 28/10/2025; Le Monde 30/10/2025; BBC 29/10/2025; AJ 29/10/2025; HRW 29/10/2025). Although offline harms are far more prevalent, the growing use of online platforms by various conflict parties underscores the need to further explore digital threats and harm.

ABOUT THIS REPORT

Aim

This report provides an overview of the types of digital threats and harms reported publicly in Sudan, highlighting the impacts on civilians and humanitarian responders. The report stresses the critical importance of understanding these harms – including weaponised disinformation, connectivity blackouts, and surveillance – because of their very real and profound offline consequences and offers concrete, illustrative examples from the Sudanese context. This report seeks to support humanitarian prioritisation, risk mitigation, and protection against digital harm. The analysis further examines how digital harm could undermine core humanitarian principles and obstruct the integrity of operations and crucial decision-making across all humanitarian clusters. It frames the compromised information environment as a new, potentially high-stakes operational front and explores effective information-as-aid intervention strategies.

Methodology

This report is based on an analysis of more than 40 publicly available sources covering issues related to digital harm, including UN and NGO publications, specialised research institutions, cybersecurity monitors, and regional and international media outlets. These sources provided insight into the nature of digital harm incidents in Sudan, allowing us to analyse them through a humanitarian action lens to better inform responses and crucial decision-making.

Limitations

Although there is an increasing focus on digital harm within the humanitarian sector, a unified, globally-agreed-upon framework to guide collective action on digital harm as a humanitarian concern is currently lacking. Digital harm is an evolving area being explored in humanitarian response, and responders may not always be aware of new or emerging threats and terminologies.

This report is based entirely on publicly available information on digital threats and harm and serves as a desk review of emerging digital harm risks in Sudan. The threats and harms highlighted in the report were identified through a thematic analysis of secondary data. Because of the focus on publicly available information, this report may exclude many digital harms that remain hidden. Additional qualitative research is critical to fully capture and contextualise digital harm in future studies.

Terminologies

Digital technologies: tools, systems, and devices that can generate, create, store, or process data (Digital Child 24/05/2022)

Doxxing: a form of cyberbullying that uses sensitive or secret information, statements, or records for the harassment, exposure, financial harm, or other exploitation of targeted individuals (Fortinet accessed 08/12/2025)

SUMMARY OF DIGITAL THREATS AND HARMS

Obstructed information access and phone and internet connectivity

Humanitarian access, operational continuity, and people's access to humanitarian assistance, services, and information often rely heavily on unimpeded phone and internet connectivity. Targeted attacks on digital infrastructure, which both warring factions in Sudan have committed, obstruct humanitarian operations and reduce affected people's ability to access aid and services that help fulfill their basic human rights. For example, a month-long nationwide communications blackout in February 2024 deprived 30 million people of phone and internet access, preventing civilians from accessing cash transfers and disrupting the coordination of emergency humanitarian aid (NRC 13/05/2024; Amnesty International 08/03/2024; ST 10/03/2024). Emergency response rooms, which rely on internet connectivity to maintain their virtual operations via WhatsApp and other social media platforms, found themselves on the verge of paralysis during the shutdown, unable to coordinate with operational responders to deliver vital food and medical supplies or operate soup kitchens (Amnesty International 08/03/2024). Communication blackouts have economic impacts on humanitarian responders if they are forced to turn to very expensive satellite services to maintain service continuity (NRC 13/05/2024). Digital disruptions also jeopardise aid access and delivery and block civilian access to life-saving information (NRC 13/05/2024; CSF 28/05/2025).

Misinformation and disinformation

Misinformation, disinformation, and hate speech online are deeply intertwined with violence offline, with harmful narratives on social media amplifying or mirroring acts of violence and sowing confusion, fear, and mistrust (CDAC 18/09/2025). Misinformation, disinformation, and hate speech fuel polarisation, undermining trust in media, hardening political divisions, fuelling real-world violence, and making postconflict reconciliation harder. Even prior to the current conflict, targeted disinformation campaigns had already undermined trust in government officials and deepened polarisation, and they have only become more prevalent (TIMEP 14/01/2025; CDAC 18/09/2025). Both SAF and RSF systematically use social media to push their respective narratives, incite and justify violence, and discredit peace advocates and women-led groups (CSF 28/05/2025; CDAC 18/09/2025). From 2023–2024, SAF, RSF, and their supporters developed and shared deepfakes and AI-generated audio content via social media to spread false information and gain sympathisers (African Arguments 23/10/2024). Coordinated troll and bot campaigns also suppress peace activists and flood X with pro-war content (LSE 16/06/2025; TIMEP 14/01/2025). RSF's social media presence and strategy are generally more advanced than SAF's, which still rely more on traditional media (TIMEP 14/01/2025). The RSF takeover of Al Fasher in October 2025 saw the use of social media platforms, including TikTok, to display the violence committed by RSF, with RSF fighters publicly admitting to killings and seemingly celebrating atrocities. AI-generated or out-of-context images and videos have also circulated, with RSF and allies exploiting these as 'fake news' to discredit reports of the atrocities they've committed. Misleading content leads to distrust in digital evidence (Beam Reports 29/10/2025 and 30/10/2025; AJ YouTube 04/11/2025). The videos of atrocities have also been used to intimidate affected communities (GPF YouTube 13/11/2025).

'Conflict monetisation' refers to for-profit networks spreading hate speech and disinformation to benefit financially from platform monetisation. A Beam Reports investigation into conflict monetisation in Sudan found that there is no single entity paying for propaganda; instead, it is an economic activity that social media platforms' own architecture enables. The Beam Reports investigation details a for-profit network of over 50 Facebook pages operated from Indonesia that systematically recycles incendiary hate speech and war propaganda from TikTok to target Sudanese audiences. Their revenue is generated directly through the platforms' built-in tools – TikTok's 'Gifts', Facebook's 'Stars', and subscriptions – turning social division into a commodity. This shadow economy is amplified by algorithms that reward divisive content with visibility, all while operating with minimal platform moderation or accountability. Conflict monetisation incentivises escalations in rhetoric, while algorithms reinforce polarised views and trap people in echo chambers – an environment where people encounter only information or opinions that reflect and reinforce their own (Beam Report 02/05/2025; GCF Global accessed 08/12/2025).

The risks associated with misinformation and disinformation extend to personal safety. For example, false claims about which areas are safe and who controls them have led civilians to delay evacuations, return to contested areas, or get caught in renewed violence. The consequences can be fatal; in Al Fasher and Zamzam camps, misleading information about safe evacuation routes opened by RSF-aligned militia resulted in civilians being killed when they attempted to flee (CDAC 18/09/2025). In the context of natural hazards, the minimisation of the severity and scale of flood risks, water contamination, food crises, and crop failure also threatens affected people's safety and wellbeing, as it can delay or hinder them from taking preventive, potentially life-saving measures or seeking support (IWMI 30/10/2024).

Misinformation and disinformation can also prevent people from accessing humanitarian services and aid. For example, inaccurate information about security incidents, aid eligibility criteria, and aid suspensions can pose barriers to people's access and erode trust in humanitarian responders (CDAC 18/09/2025). Misinformation, disinformation, and hate speech campaigns have also targeted humanitarian responders, including mutual aid groups and emergency response rooms. Commentators accuse them of collaboration with armed groups and subject them to derogatory labelling, putting aid workers at risk while simultaneously challenging the humanitarian operations' credibility. Misinformation and disinformation that claim NGOs are fuelling the continued conflict have also contributed to calls for aid organisations, especially international organisations, to be expelled from the country (Insecurity Insight 10/07/2024). This threatens the presence of humanitarian responders in conflict-affected areas.

Technology-facilitated gender-based violence

TFGBV is defined as any gender-based violence carried out or intensified through digital technologies or online platforms, including social media and gaming platforms. It can operate through phones, tracking devices using the Global Positioning System, recording devices, or drones and encompasses a range of forms, including sextortion, blackmail, cyberstalking, online sexual harassment, impersonation, hacking, hate speech, targeted campaigns, image-based abuse, technology use control, and doxxing (UNFPA 30/12/2024, 14/10/2024, and 03/2023; Conven 20/07/2025). Women and girls experiencing TFGBV in Sudan can face barriers to internet access and may decrease their online engagement to avoid violence. One qualitative study conducted in Khartoum, North Darfur, Port Sudan, and South Kordofan found that the majority of the 60 women who participated in focus group discussions did not feel safe online (APC 01/09/2023).

Prevailing gender norms mean that men in Sudan often control women's and girls' internet access; family members supervise girls, and husbands may watch their wife's online activity. In some parts of rural Khartoum, North Darfur, and South Kordofan, male family members have banned women from accessing the internet or using smartphones, believing that doing so would change their attitudes and behaviour (APC 01/09/2023). Since the conflict erupted in April 2023, RSF have used social media platforms to specifically attack women online and incite offline violence while simultaneously using intimidation to suppress dissent (SIHA 20/01/2025; Hopes and Actions 13/01/2025). Female politicians, journalists, and feminists have been subject to online defamation, causing many to withdraw from online spaces. The monitoring of internet activity can also have offline consequences; some women activists are understood to have been denied passport renewal because of their online political or media activity (Conven 20/07/2025).

Sudan has introduced two laws that may cover certain specific aspects of TFGBV: the 2018 Information Crime Law, which aims to "tackle the spread of fake news", and the 2016 amendments to the Media Law, which include clauses governing online journalism (Freedom House 01/11/2018). Sudan still does not have a comprehensive law that protects women and girls from all forms of TFGBV. Very few TFGBV survivors report online harassment out of fear of social stigma, lack of trust in the judicial system, lack of knowledge of their rights, or insufficient trust in the justice system based on previous unsuccessful attempts at legal redress in similar cases. Those who pursue justice often end up abandoning their cases after facing difficulties in providing 'conclusive' evidence. In some reported cases, survivors have done so after being accused of breaking the law themselves because of the content of the material (KACE 26/11/2020).

Child sexual abuse material

CSAM refers to any visual depiction of sexually explicit content that involves a minor (Our Rescue 10/04/2025). CSAM can be real, manipulated, or computer-generated images depicting child sexual abuse and is shared peer-to-peer or on digital sites, including common social media platforms, such as Facebook, WhatsApp, and TikTok (GPCEP accessed 20/08/2025). Chapter IX of Sudan's 2010 Child Act prohibits "the production, circulation, publication, import, export, exhibition, sale or possession" of child pornographic materials (Govt. Sudan 10/02/2010). The risk of exposure to CSAM remains, however, with at least 17,000 cases reported globally between January–June 2024 (GPCEP accessed 27/10/2025). This is likely to be a fraction of the actual number of cases, given the challenges of detecting and reporting them. CSAM data for 2025 is extremely limited. Boys and girls who have been exploited in the creation of CSAM may experience physical or psychological trauma, including post-traumatic stress disorder, feelings of shame, mental health issues, anxiety, depression, and isolation (Our Rescue 10/04/2025).